International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 5, October 2019, pp. 4266~4276
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i5.pp4266-4276

Implementation of AES using biometric

Srividya R[1], Ramesh B[2]
[1]Department of Telecommunication Engineering, K.S. Institute of Technology, India
[2]Department of Computer Science and Engineering, Malnad College of Engineering, India

Article Info

Article history:

Received Des 4, 2018
Revised Apr 25, 2019
Accepted May 4, 2019

Keywords:

AES
Biometric
MANET
Minutiae extraction
S-Box

ABSTRACT

Mobile Adhoc network is the most advanced emerging technology in the field of wireless communication. MANETs mainly have the capacity of self-forming, self-healing, enabling peer to peer communication between the nodes, without relying on any centralized network architecture. MANETs are made applicable mainly to military applications, rescue operations and home networking. Practically, MANET could be attacked by several ways using multiple methods. Research on MANET emphasizes on data security issues, as the Adhoc network does not befit security mechanism associated with static networks. This paper focuses mainly on data security techniques incorporated in MANET. Also this paper proposes an implementation of Advanced Encryption Standard using biometric key for MANETs. AES implementation includes, the design of most robust Substitution-Box implementation which defines a nonlinear behavior and mitigates malicious attacks, with an extended security definition. The key for AES is generated using most reliable, robust and precise biometric processing. In this paper, the input message is encrypted by AES powered by secured nonlinear S-box using finger print biometric feature and is decrypted using the reverse process.

Corresponding Author:

Srividya R,
Department of Telecommunication Engineering,
K.S. Institute of Technology,
#14, Raghuvanahalli, Kanakapura main road, Bangalore-109, India.
Email: srividya.ramisetty@gmail.com

1. INTRODUCTION

MANET is a wireless Adhoc Network which is dynamic in nature. It has the capability to transmit signals in between mobile nodes. Its self-configuration property essentially deals with dynamic property of moving nodes. MANET does not have organized network infrastructure in order to establish communication, because of its agility. This imposes limitations on network infrastructure, data security, processing ability, throughput and performance of the system [1]. Data security for MANET is to be designed keeping processing power and speed into consideration. Hence the deployment environment defines an extensive security at the cost of low processing power and at high data rate. MANET has on-demand need for high level security systems incorporated in network infrastructure. The literature stream lines wide number of security systems applicable to network systems. Most popular Cryptographic system illustrated in literature is advanced encryption system (AES). AES is distinguished encryption and decryption system used widely in vital computer networking applications. Key generation used to encrypt input message is again a very important aspect in data encryption/decryption systems. Use of symmetric key and asymmetric key remarks its own merits and demerits in securing data and data mobility in MANETs.

Main motivation behind data security in context of MANET is not only to secure data at high speed, but also at reduced processing power. Hence the usage of key generation is limited to implementation of symmetric key generation. However symmetric key generation is also made complex by generating the key

incorporating biometric input [2-5]. Substitution-Box (S-Box) is implemented in various methods. The most widely used method is Lookup table method. In lookup table method the hardware design counterpart is expensive in terms of resource utilization and is considered swift with moderate security. Finite field arithmetic is one of the most used approaches and it uses affine transformation. The S-box using Finite field arithmetic has high design complexity. It not only reduces computational speed but also is more expensive, compared to Lookup table method with the same security level. AES implementation is made more vulnerable with the optimization of S-box [6], which extends the security level in multiple orders. S-box design optimization confronts the security threats. However MANET systems can be made even more secure with the incorporation of enhanced features. Biometric processing is one of the most popular and extensively used techniques in the design of authentication systems. Magnitude of research is made in the respective field about the selection of features suitable for processing. Research is also done on the type and method of processing, which can be accomplished in order to define authentication. Iris, fingerprint, face, DNA and palm print recognition are a few of the features available for biometric processing. Fingerprint is considered as the most adorable and convenient approach to the context of MANET. Various techniques have been reported in literature in processing the Biometric feature extraction [7-15].

In this paper, a novel method of encryption, using Biometric as key to AES is proposed and evaluated. It is expected to overcome the limitations of existing ciphers. A Biometric based authentication technique for MANETs was described in literature [16]. This paper implements the conventional design of AES, and the key is generated using the biometric feature. Minutiae extraction is incorporated using the Morphological operational method.

In literature a paper implements biometric processing using hybrid encryption techniques [17]. The paper also illustrates its own technique in order to increase the security level in communication networks. It also discusses about symmetric and asymmetric key generation techniques. Linear behavior of S-box implementation, which is an integral functional module in AES encryption technique, was discussed in literature [6]. This paper defines greater security by incorporating nonlinearity in the implementation of S-Box.

In the paper Mixed Random 128 Bit Key Using Finger Print Features and Binding Key for AES Algorithm [18], Biometric key is used in order to encrypt plain text and decrypt cipher text. Finally the paper explains implementation of AES along with mixed key. The minutiae extraction here is accomplished using cross number approach.

The authors of the paper, Generation of 128-Bit Blended Key for AES Algorithm [19], proposed a new technique in order to generate key for AES encryption and decryption process. This paper takes iris as biometric feature and arbitrary key, to generate a blended key. The paper, Minutiae Extraction from Fingerprint Images-a Review [7], strongly recommends image quality of finger print which would essentially require less processing. Minutiae extraction on images such as binary and grey scale images at very higher glance is discussed.

The work on, Generation of Biometric Key for Use in DES [20], explains development of MANET systems using combination of Cryptographic systems and biometric key generation. Symmetric encryption technique is used, which exclusively works on non block size data. Biometric processing is incorporated in order to generate the key used for data encryption. However the data encryption strategy itself has a lot of issues in terms of key size, which is not sufficient to secure data. The paper, Minutiae extraction scheme for fingerprint recognition systems [11], distinguishes both global and local Binarization techniques. It summarizes that global Binarization is best suited for grey scale images over color images based on intensity illumination.

The neural network approach is used for minutiae extraction which is exclusively on the image without preprocessing. This paper confronts that image preprocessing would result in false minutiae extraction. The proposed technique uses series of convolution operation which results in increased latency [21].

2. RESEARCH METHOD

AES is implemented using Biometric feature for various applications. AES and Biometric processing combination ensures data security. Normally existing architectures [2-4, 8] worked on various AES and Biometric combination implementations, with respect to various applications including MANETs. Conventional AES approach is used along with morphological minutiae extraction scheme which is based on fuzzy logic. Morphological technique is used to remove spurs and noise on thinned images using HIT and Miss transforms, as these transforms require complex functions to be implemented. This morphological operation has to be performed before preprocessing and post preprocessing. It is required to be repeated twice in a row, thereby increasing total computational time. Implementation of AES using multimodal biometric

key generation is one of the known existing techniques. This implementation focuses much on multiple biometric feature extraction. Although multimodal biometric feature extraction extends security level, complexity of the design increases rapidly and will not fit into decentralized wireless architecture. AES key is also generated using mixed key input, which finds it suitable and reliable with increased security level. The mixed key is generated using fuzzy based logic which requires biometric input and random key. This again increases number of operations which consume processing power and is not suitable for battery dependent devices. MANET applications demand the architecture to be simple and secured. Hence additional computations used for extended security directly contribute to processing power complexity. Security is to be defined at the cost of fewer operations. Several encryption techniques are reported in literature which would suit MANET environment in terms of data secure mechanism. AES is considered as best approach in context with MANET. AES is recommended based on encryption time, decryption time and throughput of security system which is exceptionally remarkable over DES, Triple DES and Blowfish [22]. AES and Biometric combination is used in wide spectrum of network security applications. It is also extended to ATM machine which is designed to be high speed and also at very high security. The approach uses Biometric authentication instead of ATM card and process the information using AES and steganography technique, in order to lend cash amount. The proposed design uses AES and Biometric combination and obtains substantial results in terms of key size, time and resource consumption over DES algorithm and recommends the AES approach to applications ensuring high data security [23].

The primary objective is, to design a security technique which is best suited for MANET environment. MANET technology demands high data security in order to mitigate malicious attacks. Hence incorporating the security level is a major challenge. Security for MANET is required to be defined at the cost of high speed and less processing power. Although each of these parameters set a trade off in controlling each other, optimum solution is to be designed without compromising the performance of MANET systems. Optimum Encryption standard is to be used which defines a substantial security, retaining an optimum design complexity.

The Proposed system uses AES cryptographic system in order to secure data communication over wireless dynamic network. Symmetric key is generated using Biometric feature extraction in order to both encrypt and decrypt the data. 128 bit key is generated through Biometric feature extraction. Main focus of proposed design is in optimizing the S-box implementation, in order to increase security standard. It is followed by biometric based key generation. This combination is very popular and is considered as the best suit for MANET environment and the same is reported in literature. Figure 1 shows the proposed encryption architecture

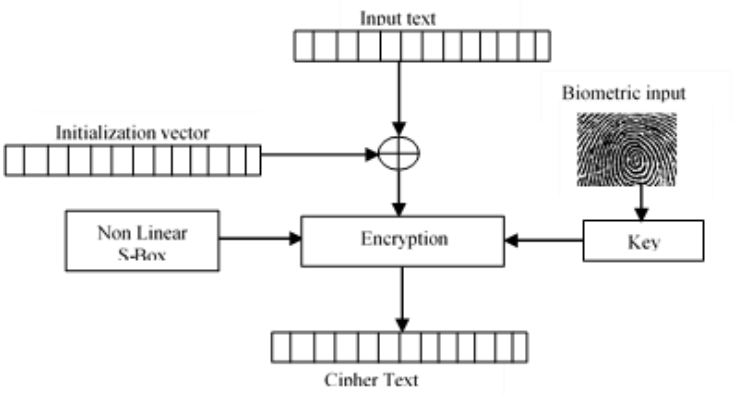


Figure 1. Proposed encryption architecture

Key for S-box is generated based on biometric features. Simple biometric feature applicable for this MANET is fingerprint. Fingerprint introduces an additional level of data security and AES key is extracted from fingerprint input. Hence it is required to use a simple and suitable biometric processing without compromising preciseness of feature extraction.

The encrypted message is cipher text and decrypted message is decipher or plain text or original message. This process is shown in Figure 2. AES is implemented and used in various data communication networks. It works with block size data which is often called as cipher text and is implemented using modified S-box which is an integral part of the encryption systems and biometric based key.

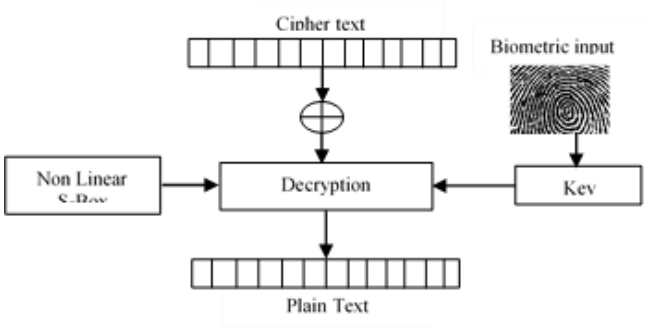


Figure 2. Proposed decryption architecture

2.1. Dynamic S-box

S-box is usually implemented using affine transformation and inverse functions in the Galio's Field GF(2^n), where n=3. This method is optimally used in various applications. Since S-box architecture is standard and would be predictable by malicious attacks. In order to add quality security to existing designs, S-box is modified by incorporating nonlinear behavior. And it would be highly difficult to predict the encryption. S-box generates a matrix of hexadecimal number and is XORed by 1's complement of the original matrix which is the base for encryption. This process is as shown in Figure 3. The same matrix is inversed at decryption end in order to retrieve the original message.

In the presented technique, input is mapped to default S-box inherently generated. Later, S-box is XORed by 1's complement of the same. It generates an intermediate S-box which is extensively nonlinear in behavior. This is responsible for generating cipher text. The intermediate S-box is inversed and is given to decryptor which generates deciphered text. Figure 4 shows Dynamic S-box used for generating cipher text.

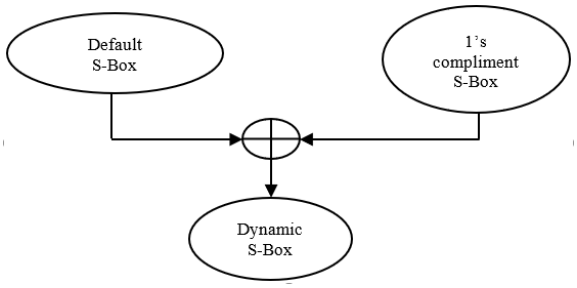


Figure 3. Dynamic S-box creation using default S-Box

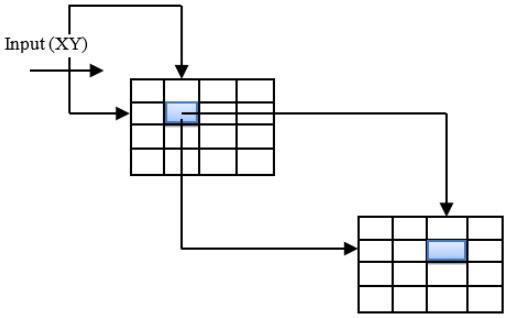


Figure 4. Dynamic S-box used for generating cipher text

In the processes of encryption, input value at the point (X, Y) is mapped to default S-box and again mapped to intermediate S-box which is responsible for generating the cipher text. As shown in Figure.4, first upper block is the default S-Box, from which values are mapped onto lower intermediate S-box finally to obtain the cipher text at some point (X,Y) in intermediate S-Box.During decryption, the cipher text is mapped to inverse of intermediate S-box and again mapped to default S-box which is responsible for generating the decipher text.

2.2. Biometric based key generation

Fingerprint is a physical trait of human beings. It is used as a biometric feature and is extracted through biometric processing. Biometric is used here to generate the key, used for data encryption and decryption. Biometric processing includes various operations such as capturing analog data, preprocessing, minutiae extraction and key generation.

Input fingerprint image is initially segmented with an intention of noise removal. The entire image is divided into matrix of size 16x16. Variance is then calculated and is compared with defined global threshold value (0.10). This is accomplished for the entire image. If the value of variance is less than threshold value,

the value is deleted. The image is later normalized to increase image quality, by obtaining desired variance. The normalized equations are shown below using (1)-(4).

$$G(i,j) = \begin{cases} M_0 + \sqrt{\frac{VAR_0\,(I(i,j)-M)^2}{VAR}}\, if\ I(i,j) > M \\ M_0 - \sqrt{\frac{VAR_0\,(I(i,j)-M)^2}{VAR}}\ Otherwise \end{cases} \quad (1)$$

where I(i,j) denotes the gray-level value at pixel (i, j). M and VAR denote the estimated mean and variance of J respectively. G(i, j) denotes the normalized gray-level value at pixel (i, j). M_0 and VAR_0 are the desired mean and variance values respectively. Image is divided into 16x16 block size. Block estimation orientation is done on the normalized image and is computed using below equations:

$$V_x(i,j) = \sum_{u=i-\frac{\omega}{2}}^{i+\frac{\omega}{2}} \sum_{v=j-\frac{\omega}{2}}^{j+\frac{\omega}{2}} 2\partial_x(u,v)\partial_y(u,v), \quad (2)$$

$$\mathrm{V_y(i,j)} = \sum_{\mathrm{u=i-\frac{\omega}{2}}}^{\mathrm{i+\frac{\omega}{2}}} \sum_{\mathrm{v=j-\frac{\omega}{2}}}^{\mathrm{j+\frac{\omega}{2}}} (\partial_{\mathrm{x}}^2(\mathrm{u,v})\,\partial_{\mathrm{y}}^2(\mathrm{u,v}), \quad (3)$$

$$\theta(\mathrm{i,j}) = \frac{1}{2}\tan^{-1}\left(\frac{\mathrm{v_y(i,j)}}{\mathrm{v_x(i,j)}}\right), \quad (4)$$

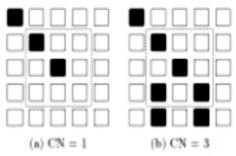
Where θ(i,j) is the least square estimate of local ridge orientation at, the block centered at pixel (i, j).

The image is binarized using Fixed Thresholding Binarization method which takes an image and returns a binary value. In this method fixed threshold value is used to assign 0's and 1's for all pixel positions. It does so by using two thresholds, one for background and one for fingerprint. The image will undergo padding with padding number of pixels from every side. Each of these padded pixels will be "painted" in black. The basic idea for fixed Binarization method is described in (5).

$$g(x,y) = \begin{cases} 1\ if\ f(x,y) \geq T \\ 0\ Otherwise \end{cases} \quad (5)$$

T shows global threshold value.

Crossing Number (CN) concept is used for minutiae extraction. By examining neighborhood of each ridge pixel using a 3x3 window. This method extracts ridge endings and bifurcations from the skeleton image. Crossing number for a pixel 'P' can be represented as in Figure 5.



P4	P3	P2
P5	P	P1
P6	P7	P8

Figure 5. Crossing number

Ridge ending pixel corresponds to a Crossing Number of one and bifurcation pixel corresponds to a Crossing Number of three. Neighborhood of P, of pixel p, as shown in Figure 5 Each minutiae points extracted from a fingerprint image is denoted as (x, y) coordinates. In this, we store those extracted minutiae points in two different vectors, Vector M1 comprises every x co-ordinate values and vector M2 comprises every y co-ordinate values. By using M1 and M2 128-bit biometric key is generated. The Algorithm for generating biometric key for BAES is stated Algorithm 1:

Algorithm 1: Generating Biometric Key

Input: Fingerprint biometric image,
Output: Biometric Key (BioKey) in Hexadecimal format
Start

1. Identify Minutiae points in RoI- NP
2. Compute modulus of the number of Minutiae points by 128, Rem -NP mod 128
3. Calculate total minutiae points available for storage, NP= NP-Rem
4. Number of interactions' J required to perform compression of the key size to 128-bit, J = NP/128
5. For 1 → J, Drop Left 64 bit and Right 64 bit. Divide the remaining key set into M_L and M_R.
6. Swap M_L and M_R
7. Convert these 128 bits to hexadecimal numbers.

Stop

The Algorithm for Biometric Advanced Encryption Standard is stated Algorithm 2:

Algorithm 2: Biometric Advanced Encryption Standard

Input: Plain text of 128 bit or 16 byte block, 16 byte BioKey
Output: Cipher-text of 128 or 16 byte bit block
Start

1. State matrix= Initial state 16 byte 4x4 matrix
2. ADDBioKey(State matrix, $BioKey_0$)
3. for rounds= 1 to n_r -1
    a. SM_s= SubstituteByte (State matrix)
    b. SM_r = RowShift (SM_s)
    c. SM_c = ColumnMix (SM_r)
    d. ADDBioKey($SM_{c,}$ $BioKey_i$)
4. SMs= SubstituteByte (State matrix)
5. SMr= RowShift (SMs)
6. ADDBioKey($SM_{r,}$ $BioKey_{nr\ -1}$)

Stop

In the above BAES algorithm SM indicates State Matrix and SMs indicates state matrix obtained after byte substitution, SMr indicates the state matrix obtained after shifting rows, SMc indicates state matrix obtained after mixing columns.

3. RESULTS AND DISCUSSIONS

AES implementation along with Biometric key generation is done on MATLAB platform. AES S-box creation logic is modified by using 1's complement method, which results in nonlinear generation of S-box and inverse S-box matrix. Hence it is highly difficult to predict the input data. This modified S-box defines an additional security thread in order to safe guard the data. The input given is a plain text which in hexadecimal format is converted to decimal data.

The decimal data, the key, modified S-box and reconfiguration matrix altogether generates a cipher text. 128 bit key is used to generate cipher text, using key expansion function. The new key matrix generated works in conjunction with S-box and reconfiguration matrix to generate the cipher text. The key used to generate cipher text is modeled by using finger print image. A Finger print image of size 256x500 is taken and is converted to grey scale as shown in Figure 6. Figure 7 shows an image which is converted to binary format using threshold comparison method. It shows an image being processed using Minutiae extraction which uses Cross number method. Extracted minutiae are converted to vectors and the vectors are again converted to 128 bit key.

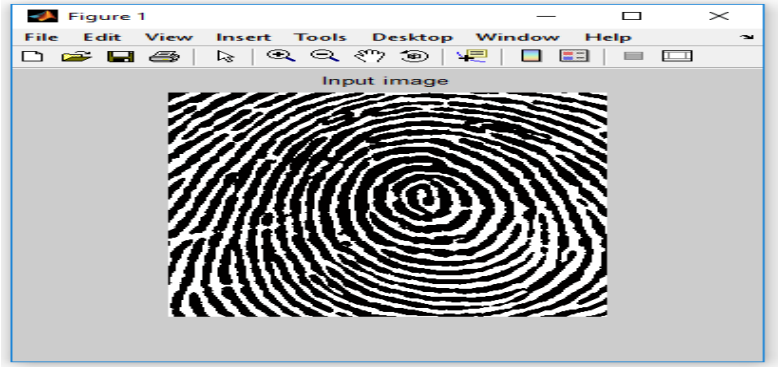


Figure 6. Input finger print image

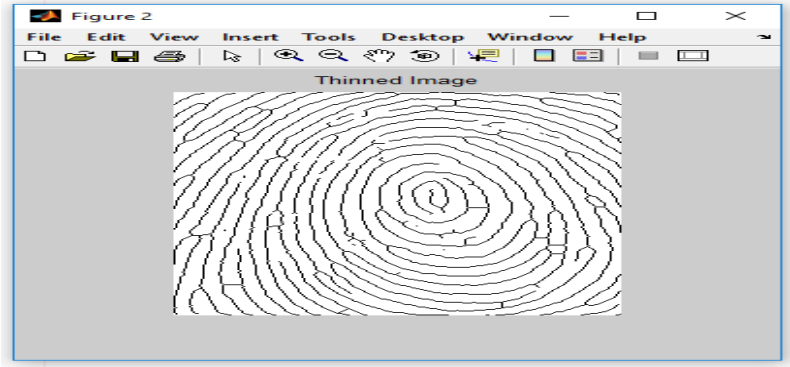


Figure 7. Binary image

The input text and Biometric processing hexadecimal key are given as shown in input text.

Input text: 0 17 34 51 68 85 102 119 136 153 170 187 204 221 238 255

The hexadecimal format of input text is shown in plaintext_hex.

Plaintext_hex = {'00' '11' '22' '33' '44' '55' '66' '77' '88' '99' ‘aa’’ ‘bb’ "cc' 'dd' 'ee' 'ff'}

Figure 8 shows Minutiae extraction point image. CN method is used in order to extract minutiae points. The 128 bit key is generated using biometric key extraction algorithm and then it is converted to hexadecimal format as shown in key_hex.

key_hex = {'1f' '3c' '2d' '01' '03' '2e' '1b' '2d' 'a4' 'c2"ff' '9a' '2b' '3a' '6e' '3f'};

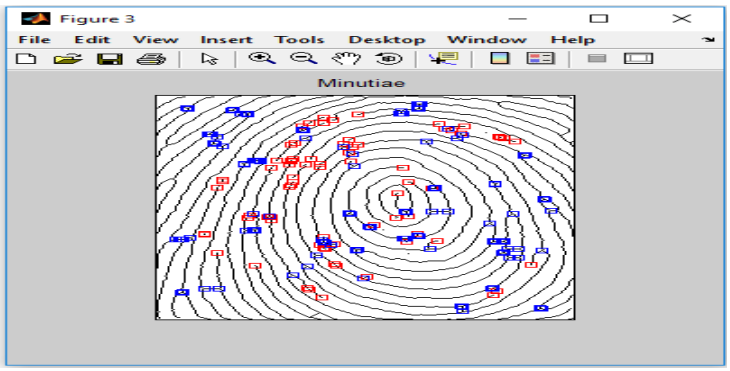


Figure 8. Minutiae extraction

Figure 9 and Figure 10 depict S-box and inverse S-Box, which are modified and used, in order to incorporate non-linear functionality.

s_box_mat =

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

Figure 9. Intermidiate S-Box

inv_s_box_mat =

82	9	106	213	48	54	165	56	191	64	163	158	129	243	215	251
124	227	57	130	155	47	255	135	52	142	67	68	196	222	233	203
84	123	148	50	166	194	35	61	238	76	149	11	66	250	195	78
8	46	161	102	40	217	36	178	118	91	162	73	109	139	209	37
114	248	246	100	134	104	152	22	212	164	92	204	93	101	182	146
108	112	72	80	253	237	185	218	94	21	70	87	167	141	157	132
144	216	171	0	140	188	211	10	247	228	88	5	184	179	69	6
208	44	30	143	202	63	15	2	193	175	189	3	1	19	138	107
58	145	17	65	79	103	220	234	151	242	207	206	240	180	230	115
150	172	116	34	231	173	53	133	226	249	55	232	28	117	223	110
71	241	26	113	29	41	197	137	111	183	98	14	170	24	190	27
252	86	62	75	198	210	121	32	154	219	192	254	120	205	90	244
31	221	168	51	136	7	199	49	177	18	16	89	39	128	236	95
96	81	127	169	25	181	74	13	45	229	122	159	147	201	156	239
160	224	59	77	174	42	245	176	200	235	187	60	131	83	153	97
23	43	4	126	186	119	214	38	225	105	20	99	85	33	12	125

Figure 10. Inverse of intermediate S-Box

The generated cipher text is shown:

105 196 224 216 106 123 4 48 216 205 183 128 112 180 197 90.

The Inverse cipher text is generated followed by decryption operation and is as shown:

0 17 34 51 68 85 102 119 136 153 170 187 204 221 238 255.

Total time taken to execute the program on MATLAB software is shown using Figure 11. Total time taken is given by 1.27097 seconds, in order to encrypt 128 bit input data with 128 bit Biometric based key and decrypt the same.

```
State at start of final round :   63 09 cd ba
                                  53 60 70 ca
                                  e0 e1 b7 d0
                                  8c 04 51 e7

After inv_shift_rows :            63 09 cd ba
                                  ca 53 60 70
                                  b7 d0 e0 e1
                                  04 51 e7 8c

After inv_sub_bytes :             00 40 80 c0
                                  10 50 90 d0
                                  20 60 a0 e0
                                  30 70 b0 f0

Round key :                       00 04 08 0c
                                  01 05 09 0d
                                  02 06 0a 0e
                                  03 07 0b 0f

Final state :                     00 44 88 cc
                                  11 55 99 dd
                                  22 66 aa ee
                                  33 77 bb ff

Elapsed time is 1.270971 seconds.
```

Figure 11. Total time taken to regenerate the decipher text

3.1. Comparative study of AES and BAES

This section gives an analysis of the proposed BAES cipher with existing AES cipher. The performance metric considered for comparison are processing time and memory utilized. Table 1 gives comparison of execution time for AES and BAES ciphers using text data input. From the table it is evident that memory utilization of BAES and AES do not vary. And BAES is equivalently efficient at the cost of minimal processing overhead.

The results are generated using MATLAB tool. Time taken could be even lesser if it is executed in fast processing systems and advanced compilers. A possible issue would be only with respect to acquiring the biometric image with high resolution and quality, and this could be addressed by using latest sensors with quality image preprocessing capability. This is a minor issue and does not majorly affect the key generation or usage.

Table 1. The comparison of AES and BAES

Parameters	AES	BAES
Memory Utilized	16kb(128bitdata)	16kb(128bitdata)
Time in sec	0.901	1.27

4. CONCLUSION

In this paper, data security technique is implemented for MANET application. The data security system is designed using amalgamation of AES and Biometric. AES is designed using unique S-box generation technique which defines multiple security levels. Key generation for encryption and decryption is incorporated using biometric input. Biometric input is a finger print image, which is easy and feasible for this context, compared to rest of the biometric profiles. Simple biometric processing technique is incorporated at the cost of optimum processing complexity.

Biometric key is preferred here since in symmetric ciphers like AES key plays a vital role and it is easy to replace the biometric key, in worst possible case if any cryptanalyst analyses the current key. The computational time is 1.270971 seconds for processing on Intel Xeon Processor with 16 GB RAM. This technique can be enhanced by properly routing the symmetric key from source node to destination node, so that additional security is accomplished. The target application of BAES could be m-governance, e-commerce, banking systems, military systems and in any genre of MANETs for secure data exchange.

REFERENCES

[1] Amol Bhosle, Yogadhar Pandey, "Applying Security to Data Using Symmetric Encryption in MANET," *International Journal of Emerging Technology and Advanced*, vol. 3, no. 1, Jan 2013.

[2] Muthukumar Arunachalam and Kannan Subramanian, "AES Based Multimodal Biometric Authentication using Cryptographic Level Fusion with Fingerprint and Finger Knuckle Print," *The International Arab Journal of Information Technology*, vol. 12, no. 5, Sep 2015.

[3] Disha Agarwal Amodini Vardhan And Pooja S., "AES Based Symmetric-Biometric Crypto System Using User Password*," Jr. of Industrial Pollution Control*, vol. 33(2), pp. 1528-1533, 2017.

[4] R.Sashank singhvi, *et al.*, "Cryptography key generation using biometrics," *2009 International Conference on Control, Automation, Communication and Energy Conservation*, 2009.

[5] Amol Bhosle, "Improving performance and securing data in manet with aes," *International Journal of Research in Advent Technology (IJRAT)*, vol. 1, no. 1, Aug 2013.

[6] E. Siva Ganesh, R. Velayutham and D. Manimegalai, "A Secure Software Implementation of Nonlinear AES S-box with the Enhancement of Biometrics," *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, IEEE, 2012.

[7] Roli Bansal, Priti Sehgal and Punam Bedi, "Minutiae Extraction from Fingerprint Images - a Review," *IJCSI International Journal of Computer Science Issues*, vol. 8, issue 5, no. 3, Sep 2011.

[8] Roli Bansal, Priti Sehgal and Punam Bedi, "Effective Morphological Extraction of True Fingerprint Minutiae based on the Hit or Miss Transform," *International Journal of Biometrics and Bioinformatics(IJBB)*, vol. 4, no. 2, 2010.

[9] Puneet and Naresh Kumar Garg, "Binarization Techniques used for Grey Scale Images*," International Journal of Computer Applications (0975 – 8887)*, vol. 71, no. 1, Jun 2013,

[10] G Vinitha Sanchez, T S Vishnu Priya, "Secure and Efficient Communication in MANETS using AES encryption and Fisheye State routing protocol," *International Journal of Innovative Research in Science, Engineering and Technology*, ISSN(Online): 2319-8753, vol. 6, no. 8, Aug 2017.

[11] D. Simon-Zorita, *et al.*, "Minutiae extraction scheme for fingerprint recognition systems," *2001 International Conference on Image Processing (Cat. No.01CH37205)* IEEE, 2001.

[12] Liu and Kai Cao, "Minutiae Extraction From Level1 Features of Fingerprint," *IEEE Transactions On Information Forensics And Security*, vol. 11, no. 9, Sep 2016.

[13] Hartwig Fronthaler, Klaus Kollreider, and Josef Bigun, "Local Features for Enhancement and Minutiae Extraction in Fingerprints," *IEEE Transactions On Image Processing*, vol. 17, no. 3, Mar 2008.

[14] Xin Gao, Xiaoguang Chen, Jia Cao, Zirui Deng, Chongjin Liu , Jufu Feng, "A novel method of fingerprint minutiae extraction based on gaborphase," *2010 IEEE International Conference on Image Processing, IEEE,* 2010.

[15] Basem O. Alijla Motaz Saad Sally F. Issawi ,"Neural Network-based Minutiae Extraction for Fingerprint Verification System," *2017 8th International Conference on Information Technology (ICIT),* IEEE, 2017.

[16] T. Priyanka, E.Ramara, "Biometric Based Authentication for MANET Using Efficient Fingerprint," *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET),* vol. 3, no. 20, Apr 2016.

[17] Mohammad Shahnawaz Nasir, Prakash Kuppuswamy, "Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 8, Oct 2013.

[18] S. Sridevi Sathya Priya, P. Karthigaikumar, "Mixed Random 128 Bit Key Using Finger Print Features and Binding Key for AES Algorithm," *2014 International Conference on Contemporary Computing and Informatics (IC3I),* IEEE, 2014.

[19] S. Sridevi Sathya Priya, P. Karthigaikumar and N.M. SivaMangai, "Generation of 128-Bit Blended Key for AES Algorithm," *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2. Advances in Intelligent Systems and Computing*, vol. 338.

[20] Rupam Kumar Sharma, "Generation of Biometric Key for Use in DES," arXiv:1302.6424, 2013

[21] Lu Jiang, *et al.*, "A direct fingerprint minutiae extraction approach based on convolutional neural networks, *2016 International Joint Conference on Neural Networks (IJCNN)*, Vancouver, BC, pp. 571-578, 2016.

[22] Umaparvathi M., Varughese D. K., "Evaluation of symmetric encryption algorithms for MANETs," *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference*, pp 1-3, 2010.

[23] Rishigesh Murugesh, "Advanced biometric atm machine with aes 256 and steganography implementation," *IEEE - Fourth International Conference on Advanced Computing, ICoAC 2012*, MIT, Anna University, Chennai, 2012.

BIOGRAPHIES OF AUTHORS

Srividya R. completed her B.E degree in Computer Science engineering and M.Tech degree in Digital Electronics from Visvesvaraya Technological University, Belgaum, India in 2009 and 2011 respectively. Currently she is working as an assistant professor in the Department of Telecommunication Engineering at Kammavari Sangham Institute of Technology, Bengaluru, India. Her areas of interest include encryption algorithms, authentication techniques, security issues in routing protocols and Mobile Ad-Hoc Networks.

Ramesh B. completed his B.E degree in computer science and engineering from Mysore University, Karnataka, India in 1991 and M.Tech degree in computer science from DAVV, Indore, Madhya Pradesh, India, in 1995 and Ph.D degree from Anna University in 2009. Currently he is working as a professor in the Department of Computer Science and Engineering at Malnad College of Engineering, Hassan, India. His research interests lie in the areas of congestion control QoS-aware routing algorithms in ad hoc networks and multimedia networks.